

# VSV Vertrauensschadenversicherung

## unterschätze Risiken

### Manche Mitarbeiter wirtschaften sehr gut – vor allem in die eigene Tasche

Vertrauen ist eine wichtige Basis für eine gute und erfolgreiche Zusammenarbeit. Leider wird man häufig enttäuscht – gerade im Arbeitsleben. Von der Datenmanipulation über fingierte Rechnungen bis hin zu Scheckbetrug: Wirtschaftskriminalität ist in deutschen Unternehmen an der Tagesordnung und eine große Gefahr für Kapital und Liquidität.

### Vielsagende Zeugen: die Zahlen

Die Millionengrenze ist längst durchbrochen: Seit 2003 registrieren deutsche Ermittlungsbehörden pro Jahr so genannte Vertrauensschäden in siebenstelliger Höhe. Von den typischen Delikten wie Betrug, Untreue und Unterschlagung waren laut einer Umfrage von KPMG in den letzten drei Jahren der mittleren Unternehmen betroffen. Die traurige Bilanz der Kriminalstatistik: Vermögensschäden im Wert von 4 Mrd. Euro allein im Jahr 2006. Nach Schätzungen der Euler Hermes Kreditversicherungs-AG werden von diesen Schäden rund 40% durch eigene Mitarbeiter verursacht. Hinzu kommt noch eine erschreckend hohe Dunkelziffer von rund 50%. Denn weil kein Unternehmen in den Ruf geraten will, dass sich seine Mitarbeiter ungehindert am Unternehmenskapital bereichern, werden viele Vertrauensschäden gar nicht erst polizeilich angezeigt.

### Sinkende Moral, steigende Schäden

In der Regel sind es persönliche Motive, die zu klassischen Vertrauensdelikten führen – zum Beispiel private Schulden oder ein Leben über die Verhältnisse. Aber auch der allgemeine Werteverfall trägt seinen Teil dazu bei. Materielle Güter werden wichtiger als Anstand, und die Schwelle zur Kriminalität sinkt.

Die Anonymisierung des Umfeldes oder zerteilte Arbeitsprozesse enden schließlich oft in fehlender Identifikation – und damit einer sinkenden Loyalität gegenüber dem Arbeitgeber.

Aber all diese Faktoren sollten nicht darüber hinwegtäuschen, dass viele Risiken im Unternehmen selbst begründet liegen.



### Vertrauen ist nötig – aber schützen kann es nicht

Vertrauensschäden können in jedem Unternehmen vorkommen, unabhängig von dessen Größe. Im klassischen Mittelstand überwiegt zumeist zwar die persönliche, vertrauensvolle Arbeitsatmosphäre – dennoch lauern auch hier Gefahren. Mitarbeiter werden häufig flexibler eingesetzt und erfüllen mehrere Funktionen. Die Folge: Sie erhalten Einblick in vertrauliche administrative Prozesse und damit Kenntnisse, die zu Fehlverhalten verleiten können – insbesondere, wenn Sicherheits- und Kontrollroutinen nicht sehr ausgeprägt sind. Ein weiterer Risikofaktor ist die EDV: Sie wird zwar hoch geschätzt, aber meist zu gering geschützt. Der Zugriff auf sensible Daten wird oft zu leichtgemacht.

## Die Ursachen für Vertrauensschäden unterscheiden sich. Die Risiken nicht.

In größeren Unternehmen sind die Verantwortlichkeiten in der Regel klar verteilt. Nur wenige Mitarbeiter sind autorisiert, mit sensiblen Firmendaten umzugehen. Schäden entstehen eher aus der steigenden Anonymität und Komplexität der Strukturen heraus. Kontrollen sind schwieriger, Sicherheitslücken bleiben unentdeckt. Häufig führen Prozesse wie Fusionen oder Reorganisationen zu Veränderungen in den gewohnten Abläufen und Zuständigkeiten. So unvermeidlich diese Anpassungen häufig sind – in puncto Sicherheit macht sich ein Unternehmen damit ein Stück weit angreifbarer. Denn dabei entstehen schnell Sicherheitslücken, die selbst vorhandene Kontrollsysteme nicht sofort schließen können.

## Jedes Netz hat Löcher – auch das digitale

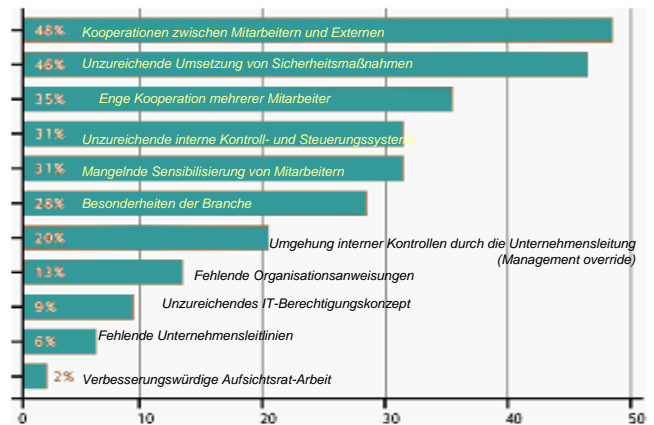
Ob Lohnbuchhaltung, Auftragsbearbeitung, Kommunikation oder Zahlungsverkehr: Informationstechnologien kommen in praktisch jedem Bereich unserer Arbeitswelt zum Einsatz. Und Sicherheitsrisiken sind damit an der Tagesordnung. Zwar ist der Zugriff auf sensible Informationen dank moderner Software häufig erschwert; ist der Zugriff aber erst einmal erfolgt, sind die Daten schnell und in großem Umfang verfügbar und können in Sekundenbruchteilen eingesehen oder modifiziert werden. So werden – zum Beispiel durch falsche Zugangsrechte – ganze Systeme manipuliert, gefälschte Daten eingegeben, Rechnungen fingiert oder Überweisungen auf das eigene Konto geleistet. Gefahr erkannt, Gefahr gebannt?

Die hohe Funktionalität von IT-Systemen verleitet häufig dazu, die Notwendigkeit wirksamer Schutzmaßnahmen im Alltag zu unterschätzen. Laut Untersuchungen von Ernst & Young glauben viele Verantwortliche, dass die Gefahr, über das Computersystem ausspioniert zu werden, gering sei.

Dabei liegen die Risiken nicht nur im eigenen Unternehmen: Gerade die Angriffe von Hackern, die sich von außen Zugang zu Ihrem System verschaffen können, richten häufig katastrophalen Schaden an.

Schutz und Kontrolle sind daher unverzichtbar. Nutzen Sie alle bestehenden Mechanismen aus. Dass besonders das Personal in Schlüsselpositionen von EDV und Systemadministration sensibel ausgewählt werden muss, ist eine Selbstverständlichkeit. Sind solche Ressourcen, wie häufig bei kleineren Unternehmen, nicht vorhanden, empfiehlt sich in jedem Fall der Einsatz eines seriösen externen IT-Dienstleisters.

## Umstände, die Mitarbeiterkriminalität begünstigen



Quelle: KPMG (Mehrfachnennungen möglich)

## Sind Sie sicher, dass Ihr Unternehmen sicher ist?

Eine KPMG-Umfrage aus dem Jahr 2006 belegt: Obwohl fast 2 von 3 Unternehmen in den letzten drei Jahren Opfer wirtschaftskrimineller Handlungen wurden, halten 77% der befragten Firmen ihre Präventionsmaßnahmen für ausreichend.

Die Einschätzung, inwieweit das eigene Unternehmen gefährdet sein könnte, bleibt also offenbar hinter der Realität zurück. Das wirft die Frage auf, wo die immensen Schäden wirklich entstehen – und warum die Gefahr offensichtlich so selten erkannt wird.

## Das Wesen jeden Schadens: Sichtbar wird er erst, wenn es zu spät ist.

Interne Kontrollsysteme decken dabei noch immer den größten Teil aller Vertrauensschäden auf – ganz gleich, wo die Täter sitzen. An zweiter Stelle jedoch folgt der Faktor Zufall und spielt damit eine weitaus wichtigere Rolle bei der Aufklärung von Fällen als interne oder externe Hinweise, als Polizei oder Staatsanwaltschaft.

Völlig machtlos ist allerdings kein Unternehmen: Es gibt Warnsignale, auf die Sie als Verantwortlicher achten können. Zu diesen Anzeichen für eine mögliche Veruntreuung gehören:

- Veränderung im Verhalten oder im Lebensstil von Mitarbeitern.
- Ungewöhnliches Wachstum/ein ungewöhnlich hoher Auftragsbestand.
- Inventurdifferenzen.
- Ungewöhnliche finanzielle Entwicklung des Unternehmens.
- Unzufriedenheit bei Vorgesetzten bzw. Mitarbeitern.
- Hinweise von Mitarbeitern.

## Ihre guten Mitarbeiter machen was Sie wollen – die anderen machen was sie wollen.

Ein wirksames Risk Management erfordert nicht zwangsläufig einen hohen Aufwand – aber es verlangt Aufmerksamkeit an den entscheidenden Punkten. Vorbeugung bedeutet auch Abschreckung. Und vorbeugen kann jeder.

## Das wichtigste Kapital: Ihre Mitarbeiter

Vertrauen Sie bei der Auswahl neuer Mitarbeiter nicht nur persönlichem Eindruck und Fachkompetenz. Schauen Sie sich Arbeitszeugnisse und Papiere gründlich an, fragen Sie bei Unklarheiten nach. Lücken im Lebenslauf sollten plausibel erklärt werden. In manchen Fällen kann es ratsam sein, ein polizeiliches Führungszeugnis einzuholen. Bedenken Sie zudem, dass die Loyalität zum Unternehmen bedeutend höher ist, wenn die Mitarbeitermotivation stimmt!

## Vertrauen ist gut, Kontrolle ist besser

Beachten Sie konsequent das Vier-Augen-Prinzip. Das heißt: Die zweite Unterschrift sollte keinesfalls nur dekorativen Charakter haben. Das Risiko verringert sich deutlich, wenn eine kontrollierende Instanz vorhanden ist – und das eben nicht nur in der Theorie. Diese Regel gilt auch für den digitalen Datenfluss!

## Geldflüsse organisieren

Im Umgang mit Geld gilt die Regel: möglichst keine Schecks! Zu leicht lassen sich hier Einträge ändern oder Vordrucke mit gefälschter Unterschrift ausfüllen. Zudem nehmen gerade ausgehende Schecks häufig einen langen Weg durch die Abteilungen – eine Kontrolle ist damit erheblich erschwert.

## Arbeitsbereiche klar definieren

Sorgen Sie dafür, bestimmte Unternehmensbereiche klar zu trennen: die Finanz- und Debitoren-

buchhaltung, die Kasse und den Verkauf. Schaffen Sie exakt ausgearbeitete Arbeitsplatzstrukturen. Kompetenzen und Funktionen müssen klar aufgeteilt, Jobs genau beschrieben und Arbeitsabläufe eindeutig definiert sein.

## Sensibel für ungewöhnliche Entwicklungen

Bewahren Sie sich einen sensiblen Blick für die Stimmigkeit im Lebensstil Ihrer Mitarbeiter. Nicht jede Veränderung der Lebensverhältnisse ist gleich ein Anzeichen für Veruntreuung; bei ungewöhnlichen Abweichungen allerdings sollten Sie aufmerksam werden.

*Die eigene Risikobewertung:  
Optimismus wider besseres Wissen?*

*62% der Unternehmen meinen, dass Wirtschaftskriminalität in nächster Zeit steigen wird, aber nur 32% der Unternehmen schätzen das Risiko, selbst Opfer zu werden, als „eher hoch“ oder „sehr hoch“ ein.\*  
77% halten die eigenen Präventionsmaßnahmen für ausreichend, aber lediglich 18% der Befragten mit dieser Ansicht bezeichnen die eigene Kenntnis wirtschaftskrimineller Handlungsmuster als gut.\*  
Im Durchschnitt schätzen Manager die Dunkelziffer im eigenen Unternehmen nur rund halb so hoch ein wie in der Gesamtheit ihrer Branche.*

*\* Quelle: KPMG*

## **Pflicht: regelmäßige Bestandsaufnahmen**

Inventuren kosten viel Zeit und sind personalintensiv. Nichtsdestoweniger sind sie ein besonders geeignetes Mittel, um Veruntreuung oder Diebstahl aufzudecken. Führen Sie daher routinemäßig Inventuren durch.

## **Wenn der Ernstfall da ist: Schnell und konsequent handeln**

Veruntreuungen geschehen trotz aller Vorsichtsmaßnahmen. Setzen Sie dann deutliche Zeichen und schalten Sie Polizei und Staatsanwaltschaft ein. Noch besser aber ist: Warten Sie nicht auf den Schadenfall. Ergänzen Sie Ihr Sicherheitskonzept, durch eine Vertrauensschadenversicherung.

## **Verlassen Sie sich nicht nur auf Ihre Menschenkenntnis. Sondern auf finanzielle Sicherheit im Ernstfall.**

Kommt es trotz aller Vorsichtsmaßnahmen zu einem Vertrauensschaden, ist das Geld meist so gut wie verloren – auch, wenn der Täter feststeht: Nach einer Studie von PWC konnten 73% der befragten Unternehmen nicht mehr als 20% ihres finanziellen Schadens zurückführen – viele gingen sogar ganz leer aus!

Der Versicherungsvertrag wird nach Ihren individuellen Bedürfnissen gestaltet; die Höhe der Prämie richtet sich nach der Versicherungssumme, der Anzahl der versicherten Personen sowie nach der Laufzeit des Vertrages.

## **Die Schadenregulierung**

Wenn der Schädiger namentlich ermittelt und dessen Haftung nachgewiesen ist, beginnt die Schadenregulierung durch den Versicherer. Aber auch, wenn der Täter nicht namentlich identifiziert wurde, haben Sie Anspruch auf Leistung:

Voraussetzung ist lediglich, dass sich aus dem Sachverhalt und den Ermittlungen ergibt, dass der Schaden mit überwiegender Wahrscheinlichkeit vorsätzlich durch eine Vertrauensperson verursacht wurde. Die Versicherung nimmt Ihnen das Risiko ab, dass der Täter nicht in der Lage ist, den Schaden zu ersetzen.

## **Was ist versichert?**

- *Vermögensschäden, die von Betriebsangehörigen und anderen Vertrauenspersonen vorsätzlich verursacht werden, bis zu zwölf Monate nach deren Ausscheiden.*
- *Schäden durch Diebstahl, Unterschlagung, Betrug (einschließlich Computerbetrug), Geheimnisverrat, Untreue oder andere vorsätzliche unerlaubte Handlungen, die zum Schadenersatz verpflichten (z. B. Sachbeschädigung oder Sabotage).*
- *Schäden, die Dritten durch Ihre Mitarbeiter vorsätzlich zugefügt werden.*
- *Schäden durch sogenannte Hacker (für EDV/IT). Täuschungsschäden durch außenstehende Dritte.*
- *Unmittelbare Vermögensschäden sind bis zur Höhe der Versicherungssumme gedeckt.*
- *Externe Schadenermittlungs- und Rechtsverfolgungskosten werden bis zu 20% des versicherten unmittelbaren Schadens im Rahmen der Versicherungssumme übernommen sowie zusätzliche interne Schadenermittlungs- und Rechtsverfolgungskosten.*

## **Auf wen bezieht sich die Versicherung?**

*Auf alle Arbeitnehmer, Angestellten, Aushilfen, Praktikanten, online tätigen Mitarbeiter außerhalb der Geschäftsräume („Home-Office“), Zeitarbeitskräfte und Fremdpersonal. Auf Geschäftsführer und Vorstandsmitglieder mit maximal 20 % Anteilsbesitz. Aufsichtsräte, Verwaltungsräte und Beiräte. Auf alle Unternehmen weltweit, an denen Sie mehrheitlich beteiligt sind.*

**AsseCon Assekuranzmakler GmbH - Leopoldstr. 70 - 80802 München -  
Tel. 089/343 878 - Fax 089/343 979 [www.assecon.de](http://www.assecon.de) eMail: [mbo@assecon.de](mailto:mbo@assecon.de)  
Sitz der Gesellschaft: München - Handelsregister München HRB 96356 Geschäftsführer: Manfred Bock**

Pflichtangaben nach EU-Vermittlerrichtlinie:

AsseCon ist ein unabhängiger Versicherungsmakler mit Erlaubnis nach § 34 d Abs. 1 Gewerbeordnung. Es bestehen keine Beteiligungen von oder an Versicherungsunternehmen. Zuständige Erlaubnisbehörde: IHK München; Max-Joseph-Straße 2; 80333 München; Tel.: 089/5116-0 **Registernummer:** D-RO3-LR-IVAS-26 Die Eintragung im Vermittlerregister kann überprüft werden: DIHK e.V. · Breite Straße 29 · 10178 Berlin · Tel. 030/20308-0 ·